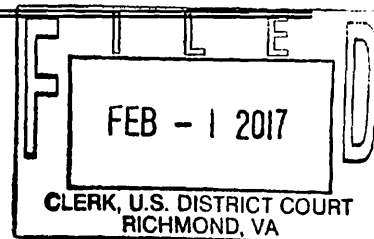


UNITED STATES DISTRICT COURT

for the
Eastern District of Virginia

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

6800 Paragon Place
Suites #430 and 440
Richmond, Va. 23230

Case No. 3:17 ~~MS~~ SW9

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

6800 Paragon Place, Suites #430 and 440, Richmond, Va. 23230

located in the Eastern District of Virginia, there is now concealed (identify the person or describe the property to be seized):

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☐ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
18 U.S.C. § 1343

Wire Fraud

Offense Description

The application is based on these facts:

See attached affidavit, incorporated as if stated herein.

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Sworn to before me and signed in my presence.

Date: January 31, 2017

City and state: Richmond, Va.

Applicant's signature

S.A. Joseph Quinn, Federal Bureau of Investigation

Printed name and title

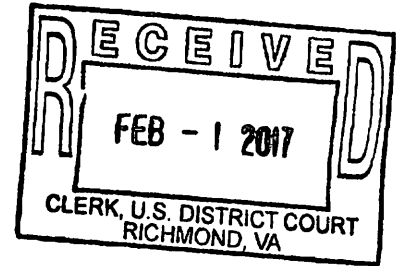
/s/
David J. Novak
United States Magistrate Judge

Judge's signature

The Hon. David J. Novak, U.S. Magistrate Judge

Printed name and title

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division**



IN THE MATTER OF THE SEARCH OF:)
The property located at) Crim. No. 3:17SW9
6800 Paragon Place)
Suites #430 and 440)
Richmond, Va. 23230)

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, Joseph P. Quinn, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for the offices of Trust Title Services LLC, located at 6800 Paragon Place, Suite #440, Richmond, Virginia, 23230, and Trust Mortgage Corporation LLC, located at 6800 Paragon Place, Suite #430, Richmond, Virginia, 23230, in the Eastern District of Virginia. The locations to be searched are described in the following paragraphs and in Attachment A, incorporated herein by reference.

2. I have been employed as a Special Agent of the Federal Bureau of Investigation (FBI) for over 17 years. I have primarily investigated criminal matters concerning violations of federal laws commonly referred to as “white collar crimes,” such as financial institution fraud, investment fraud, securities fraud, mortgage fraud, fraud by wire and mail fraud (18 U.S.C. §§ 1341 *et seq.*). I have executed numerous search warrants and have made numerous arrests throughout my career as a law enforcement officer. As a Special Agent of the FBI, I am authorized to investigate violations of federal law and submit this affidavit.

3. The facts set forth in this affidavit are based on my personal participation in this investigation and from information provided by an FBI forensic accountant, state regulators,

victim-witnesses, and on my experience, training, and background as a FBI Special Agent. I have not included every fact known to me or the United States concerning this investigation and have set forth only the facts necessary to support probable cause for this action.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 1343 have been committed by Roberto Jaramillo (Jaramillo) and others as yet unknown. There is also probable cause to search the locations described in Attachment A for evidence and instrumentalities of these crimes as further described in Attachment B.

PROBABLE CAUSE

5. This investigation is being worked jointly by the FBI and the Federal Housing Finance Agency, Office of the Inspector General. Based on my investigation to date, there is probable cause to believe that Jaramillo and others have participated in a scheme to defraud using interstate wires, in violation of Title 18, United States Code, Section 1343, and that business records and other items that have been used in furtherance of the scheme will likely be found at Jaramillo's business, Trust Title.

Background

6. At all times relevant to this affidavit, Jaramillo was the owner of Trust Mortgage Corporation LLC ("Trust Mortgage"). Virginia State Corporation Commission records show that Trust Mortgage was formed on December 3, 2007. On July 9, 2013, Jaramillo, registered agent, changed the office location from 5516 Falmouth Street, Suite 301A, Richmond, VA, to 6800 Paragon Place, Suite 430, Richmond, VA.

7. At all times relevant to this affidavit, Jaramillo was also the owner of Trust Title Services LLC ("Trust Title"). Virginia State Corporation Commission records show that Trust

Title was formed on December 1, 2010. On July 9, 2013, Jaramillo, registered agent, changed the office location from 5516 Falmouth Street, Suite 301, Richmond, VA, to 6800 Paragon Place, Suite 440, Richmond, VA.

8. At all times relevant to this affidavit, Jaramillo was a licensed mortgage broker with the Commonwealth of Virginia.

9. Starting sometime in September 2015 and continuing to June 2016, Jaramillo used his positions at Trust Mortgage and Trust Title in a scheme to divert loan proceeds for personal and business expenses. Although investigators have not finished reviewing bank records related to Jaramillo and these entities, I have observed extensive comingling of borrowed funds, other capital, operating expenses, and Jaramillo's personal expenses.

10. In sum, I believe that the scheme involved client borrowers who obtained loans from Trust Mortgage or brokered them through Trust Mortgage, which then would close at Trust Title. Trust Title had an obligation to pay the lien holders with the proceeds of the loans obtained by the borrowers. Jaramillo did not pay the lien holders—but rather diverted the funds from Trust Title to Trust Mortgage and used them to pay his personal and business expenses. Until in or about June 2016, I believe that Jaramillo operated, in essence, a Ponzi scheme in which he used funds from new incoming client borrowers to pay off old lien holders, either in monthly payments or a payment of the final loan payoff amount.

JD's Refinance Loan

11. For example, in or about January 2016, "JD" had an existing mortgage on XX Fieldstone Road, Richmond, VA, 23234, from Carrington Mortgage Services. As of in or about January 12, 2016, the outstanding balance on the mortgage was \$161,864.94.

12. JD sought to refinance the loan and obtained a refinance loan from Platinum Mortgage through Trust Mortgage, which was supposed to close at Trust Title on or about January 7, 2016.

13. On or about January 12, 2016, Platinum Mortgage wire transferred \$167,695.33 into Trust Title account -8633. Jaramillo and L.G., an employee of Trust Title, are the signatories on Trust Title account -8633. JD understood that these funds would be used to pay Carrington Mortgage Services' lien on JD's home and other expenses related to JD's real estate settlement.

14. Instead, Trust Title account -8633 instead transferred the \$161,864.94 to Trust Mortgage's account -8512 on or about January 14, 2016. Jaramillo was the only signatory on the Trust Mortgage account -8512. The transaction detail in the Trust Title bank statement falsely lists the beneficiary as Carrington Mortgage Services when, in truth and fact, the money was going to Trust Mortgage's account -8512. In this account, the \$161,864.94 was comingled with approximately \$151,000. From in or about January 14 to February 11, 2016, the funds were depleted from checks drawn on the account (unknown purposes), payroll expenses, normal business expenses and \$36,000 in a transfer to Jaramillo's personal bank account.

15. After January 7, 2016, in an apparent effort to keep JD's monthly mortgage payments current, Trust Title made six periodic payments of \$1,296.98 to Carrington Mortgage Services via ACH transfers. These payments came from Trust Title's account -1215, on which Jaramillo was the sole signatory.

16. Ultimately, JD's loan from Carrington Mortgage Services was never paid off with the refinance loan from Platinum Mortgage, as JD expected. Rather, on July 29, 2016, Title

Insurance Company A paid \$160,814.83 to Carrington Mortgage Services to settle the lien. Title Insurance Company A subsequently filed a civil lawsuit against Jaramillo.

JP's Refinance Loan

17. As another example, in or about April 2016, "JP" had an existing mortgage on XX Tulane Avenue, Richmond, Virginia, 23226, from PNC Bank. As of in or about April 27, 2016, the outstanding balance on the mortgage was \$195,372.72. In addition, JP had a line of credit of approximately \$21,237.36 from DiTech Financial LLC.

18. JP sought to refinance these loans and obtained a refinance loan through Trust Mortgage, which was supposed to close at Trust Title on or about April 27, 2016. Platinum Mortgage was the lender for JP's refinance loan of \$224,438.65.

19. On or about April 27, 2016, Platinum Mortgage transferred JP's refinance loan, \$224,438.65, by wire to Trust Title account -8633, on which Jaramillo and L.G., an employee of Trust Title, are the sole signatories. Based upon the escrow documents, these funds would be used to pay off his existing PNC Bank mortgage and the DiTech Financial LLC line of credit.

20. On or about April 28, 2016, Title Trust transferred \$21,237.36 from account - 8633 to DiTech Financial LLC to pay off JP's line of credit.

21. Trust Title did not pay off JP's existing mortgage with PNC Bank. Instead, on or about April 28, 2016, the remaining balance of the refinance loan was transferred to Trust Mortgage account -8512, on which Jaramillo was the only signatory. The \$195,372.72 was comingled with approximately \$121,000. For the following six weeks, these funds were used to pay payroll expenses, business expenses, and \$42,000 in transfers to Jaramillo's personal bank account.

22. During this six-week time period, the monthly mortgage payments on XX Tulane Avenue to PNC Bank were maintained by withdrawals from Jaramillo's personal Wells Fargo Bank account.

23. In early June 2016, Platinum Mortgage discovered that the prior lien holder for a refinance transaction closed at Trust Title was not paid off as expected. On or about June 13, 2016, Platinum Mortgage contacted Trust Title and requested proof that the prior lien holder was paid off. On or about June 14, 2016, Platinum Mortgage spoke with Jaramillo and requested a copy of the wire that was sent to pay off the lien in question. On or about June 14, 2016 Platinum Mortgage informed Title Insurance Company A about Trust Title's failure to pay a prior lien holder. After June 14, 2016 Platinum Mortgage and Insurance Company A conducted an audit of transaction which closed at Trust Title and discovered additional transaction in which the prior lien holder was not paid off. Platinum Mortgage questioned Jaramillo about the additional transactions.

24. As of June 14, 2016, the balance on the PNC Bank mortgage on XX Tulane Avenue was \$194,339.82 and the Trust Mortgage account -8512, on which Jaramillo was the only signatory, had only \$94,807.95.

25. On June 15, 2016—after Jaramillo was questioned by Platinum Mortgage—Trust Title transferred the proceeds of loans from four other Trust Mortgage clients ("RC" for \$108,357.00; "NC" for \$178,324.91; "HA" for \$143,792.39; and "MU" for \$239,914.48) into Trust Mortgage account -8512. As such, the Trust Mortgage account -8512 now had approximately \$765,196.73.

26. On June 17, 2016, Trust Mortgage transferred funds from account -8512—on which Jaramillo was the only signatory—to PNC Bank to pay off the \$194,339.82 balance of JP's mortgage at PNC Bank.

27. At around that same time, Trust Mortgage transferred funds from account -8512—on which Jaramillo was the only signatory—to make payoffs for three other lien holders who should have been paid several months prior to June 2016. For example, on June 16, 2016, the account paid \$111,753.49 for a loan with an original closing date of March 25, 2016; on June 20, 2016, the account paid \$120,034.50 for a loan with an original closing date on September 25, 2015; and the account paid \$102,221.98 for a loan with an original closing date on February 22, 2016.

28. In addition, from June 15 to June 30, 2016, Trust Mortgage account -8512—on which Jaramillo was the only signatory—withdrew \$70,000 for payroll and taxes and transferred \$155,000 to Jaramillo's personal account. The balance in the Trust Mortgage account -8512 on June 30, 2016 was \$14,902.48.

Other Loans

29. Starting in September 2015 and continuing to June 2016, I have observed 8 transactions in which Trust Title failed to pay off the lien holder in first position in a timeframe consistent with an escrow closing. I have obtained documents and records that show that Trust Title failed to pay off the lien holder in first position in a timeframe consistent with escrow closings for 8 transactions, including the two transactions detailed above (JD and JP) and a refinance loan for Jaramillo's personal residence. For all of the 8 transactions, the funds representing the proceeds of the loan, which should have been used to pay the lien holders, were transferred from Trust Title accounts to Trust Mortgage accounts. Five of the lien holders were

eventually paid off from Trust Title or Trust Mortgage accounts several months after the date of escrow. Two of the lien holders were paid off by Title Insurance Company A.

30. Trust Title ceased doing business in or about June 23, 2016.

Trust Title Interviews

31. On or about June 29, 2016, the Virginia Bureau of Insurance interviewed Jaramillo and several Trust Title employees. One employee told investigators that Jaramillo had final approval authority for all escrow disbursements. Another former employee stated that only Jaramillo was authorized to wire funds for settlement transactions. She became frustrated with Jaramillo when she questioned Jaramillo about the missing funding deposits and he provided unsatisfactory answers.

32. On or about January 5, 2017, your affiant interviewed Jaramillo. He admitted that monies and loan proceeds were transferred from Trust Title to Trust Mortgage's operating account, instead of paying off lien holders as expected. Jaramillo also admitted he used these operating expenses for his business. Jaramillo claimed, however, that this all occurred "accidentally." He told your affiant that he and employee L.G. both had to approve outgoing wires from Trust Title after a settlement, but Jaramillo professed to have no understanding about how funds were misdirected.

33. Jaramillo also stated that he is currently working for Paramount Residential Mortgage Group (PRMG) as an area manager, a position that he started in November or December of 2016. PRMG is located in the same office space in which Trust Mortgage was located and, as further described in Attachment A, the building signage includes both "Trust Mortgage" and "PRMG." Jaramillo told your affiant that the Trust Title computers and server are currently in the office space and that Trust Title's information is located on the server.

Computers and the Internet in Relation to the Fraud

34. Your affiant has been involved in fraud investigations for several years. Through this experience, and based upon my own personal observations and information supplied to me by other law enforcement officers and bank fraud investigators, your affiant knows the following:

a. In the modern business environment, with financial intuitions, large companies, and merchants, use of computers and the Internet have become a standard method by which companies conduct commerce, business transactions and maintain/store critical information.

b. In the modern business environment, I know that businesses such as Trust Title should have an established record retention policy. I have confirmed with the Virginia State Corporations Commission, Bureau of Insurance, that businesses that operate as title and settlement agents, such as Trust Title, must retain settlement records for five years after the date of settlement (the retention requirement for title agents who do not conduct settlements is three years). One of the reasons for maintaining business records according to a record retention policy would be to satisfy the Internal Revenue Service in the event of an audit. The following are generally accepted record retention guidelines for business records: bank statements (3 years); cancelled checks (7 years); invoices (7 years); accounts payable and receivable ledgers (7 years); contracts, mortgages, notes, and leases (7 years); general correspondence (2 years); legal and other important correspondence (permanently); financial statements (permanently); minute books (permanently); payroll records (7 years); property records (permanently); tax returns and work papers (permanently); training manuals (permanently).

c. In addition, the use of electronic mail (email) has become commonplace for business and personal use. Email is extensively used for communicating with financial industries, service providers, merchants, clients and for personal use. Almost all financial institutions and merchants have an Internet presence of some sort, usually in the form of a public web page. In this case your affiant knows that Trust Title has a website under www.trusttitleservices.com.

d. Accordingly, computer hardware, software, documentation, passwords, and data security devices may be important to a criminal investigation in two distinct and important respects: (1) those objects themselves may be instrumentalities, fruits, or evidence of crime, and/or (2) those objects may have been used to collect and store information about crimes (in the form of electronic data). Rule 41 of the Federal Rules of Criminal Procedure permits the Government to search and seize computer hardware, software, documentation, passwords, and data security devices that are (1) instrumentalities, fruits, or evidence of crime, or (2) storage devices for information about a crime.

e. The computer's capability to store data and manipulate images and documents in a digital form makes it an ideal repository for committing fraud.

f. On or about January 5, 2017, Jaramillo told law enforcement that his computers and server are still located within Trust Title. He stated that Trust Title's information is located on the server. He also said that he uses Excel spreadsheets to keep track of his financial statements.

g. On January 25, 2017, your affiant visited office building where Trust Title and Trust Mortgage have office space. Suite #430 is now labeled as "PRMG" and Suite #440 has no label. Suites #430 and #440 share a reception area and have a common entrance. At

11:25 am on January 25, 2017, I observed Jaramillo in a conference room connected to the reception area. As detailed above, Jaramillo was interviewed on January 5, 2015. During the interview Jaramillo stated that the Trust Title computers server were located at the office suite. During the interview Jaramillo stated that he worked at PRMG. Based on my observations, PRMG occupies the same office space as Trust Mortgage.

35. Based on the foregoing, I respectfully submit that there is probable cause to believe that Roberto Jaramillo engaged in a scheme and/or artifice to defraud using interstate wires, in violation of Title 18, United States Code, Section 1343, and that Trust Title currently contains business records in the form of hard copy documents and computerized records, and other items described in Attachment B below, related to such violations.

TECHNICAL TERMS

36. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

b. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

37. As described above and in Attachment B, this application seeks permission to search for records that might be found at the search locations, in whatever form they are found.

One form in which the records might be found is data stored on a computer's hard drive or other storage media, including a cellular or mobile telephone. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

38. *Probable cause.* I submit that if a computer or storage medium is found at the search locations, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. Depending on a variety of factors, a particular computer could easily not overwrite deleted files with new data for many months, and in certain cases conceivably ever.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic

evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

39. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the search locations because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, “chat,” instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic

programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

40. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on

the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

41. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of computers and other electronic storage media consistent with the warrant. The examination may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

**SPECIFICITY OF SEARCH WARRANT RETURN AND NOTICE
REGARDING INITIATION OF FORENSIC EXAMINATION**

42. Consistent with the Court's current policy, the search warrant returns will list the model(s) and serial number(s) of any and all computers or other electronic storage media seized at the search locations, and include a general description of any and all associated peripheral equipment that has been seized.

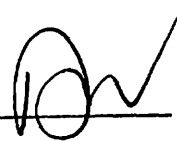
43. Moreover, the Government will file a written pleading in this case within one hundred twenty (120) days after the execution of the search warrant notifying the Court that the imaging process of digital evidence seized from the target locations is complete, and the forensic analysis of any devices has begun. Such notice will include confirmation that written notice has been provided to the defendant or his counsel informing the defendant that the forensic

examination of evidence seized from him has actually begun. Such notice to the defendant and the Court is not intended to mean, and should not be construed to mean, that the forensic analysis is complete, or that a written report detailing the results of the examination to date will be filed with the Court or provided to the defendant or his counsel. This notice does not create, and is not meant to create, additional discovery rights for the defendant. Rather, the sole purpose of this notice is to notify the defendant that, beyond the simple seizure of his property, a forensic search of that property has actually begun.



Joseph P. Quinn., Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me
This 31 day of January, 2017.


/s/
David J. Novak
United States Magistrate Judge

ATTACHMENT A
Locations to Be Searched

This affidavit is submitted in support of a search warrant for the following locations:

The location is 6800 Paragon Place, suites 430 and 440, Richmond, Virginia, 23230, in the Eastern District of Virginia, and is further described as office suites located within the Paragon Place office building, which is a large six story glass and stone office building. The office building contains a sign in the elevator lobby which list suite #430 as Trust Mortgage and suite #440 as Trust Title. Suite #430 and 440 share a common entrance. Glass doors close the suites off from the elevator lobby. The suites share a reception area. Suite #430 is now labeled as PRMG and Suite #440 has no label. Suites #430 and 440 share a reception area and have a common entrance.

ATTACHMENT B
Description of Items to Be Seized

Evidence, fruits and instrumentalities relating to violations of 18 U.S.C. § 1343 (Wire Fraud), more particularly described as:

1. Records and items related to Trust Title, Trust Mortgage, Roberto Jaramillo, or any other business owned, operated or incorporated by Jaramillo, using their true name or any alias names, which constitute evidence, fruits, or instrumentalities of violations of Title 18, United States Code, Section 1343, including but not limited to the following:
 - a. All business ownership and operational records, including but not limited to: articles of incorporation, business licenses, federal and state tax returns, state sales tax records, contracts, mortgages, notes, leases, lists/contact information for suppliers and vendors, telephone records, travel documents and receipts, appointment calendars, correspondence, website administration, etc.;
 - b. All records and documents related to financial transactions, including but not limited to: bank statements, cancelled checks, check stubs, wire transfer records, check books/registers, credit card statements, money orders, and other items identifying sources of income and expenditure;
 - c. All cash or monetary instruments signed by or issued to Trust Title, Trust Mortgage, Roberto Jaramillo, or any other business owned, operated or incorporated by Jaramillo, using their true name or any alias names; for the purpose of seizure, all U.S. currency will be seized only if \$3,000.00 or more is located;
 - d. All personnel and payroll records reflecting any persons employed on a full-time, part-time or contract basis at any time, including social security numbers, addresses, phone numbers, birth dates, job descriptions and dates of employment;
 - e. Any and all records, either paper or electronic, relating to the website www.trusttitleservices.com.

Computers and Storage Medium

2. This warrant authorizes the seizure and search of any computers or storage medium capable of being used to commit, further, or store evidence of the offenses listed above. Mirroring, imaging, and/or replication are also authorized.
3. For any computer or storage medium whose seizure and search is authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

f. evidence of the times the COMPUTER was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

i. records of or information about Internet Protocol addresses used by the COMPUTER;

j. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

k. contextual information necessary to understand the evidence described in this attachment.

l. Routers, modems, and network equipment used to connect computers to the Internet.

m. As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

n. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or

storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

o. The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.